(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 January 2001 (25.01.2001)

PCT

(10) International Publication Number
WO 01/06726 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US00/18988

(22) International Filing Date: 12 July 2000 (12.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/354,294 15 July 1999 (15.07.1999) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventors: JOHNSON, John; 1061 Regency Knoll Drive, San Jose, CA 95129 (US). OKIN, Ken; 14880 Sobey Road, Saratoga, CA 95070 (US). RADUCHEL, William; 3111 Alexis Drive, Palo Alto, CA 94304 (US).

(74) Agent: KIVLIN, B., Noel; Conley, Rose & Tayon, P.C., P.O. Box 398, Austin, TX 78767-0398 (US).

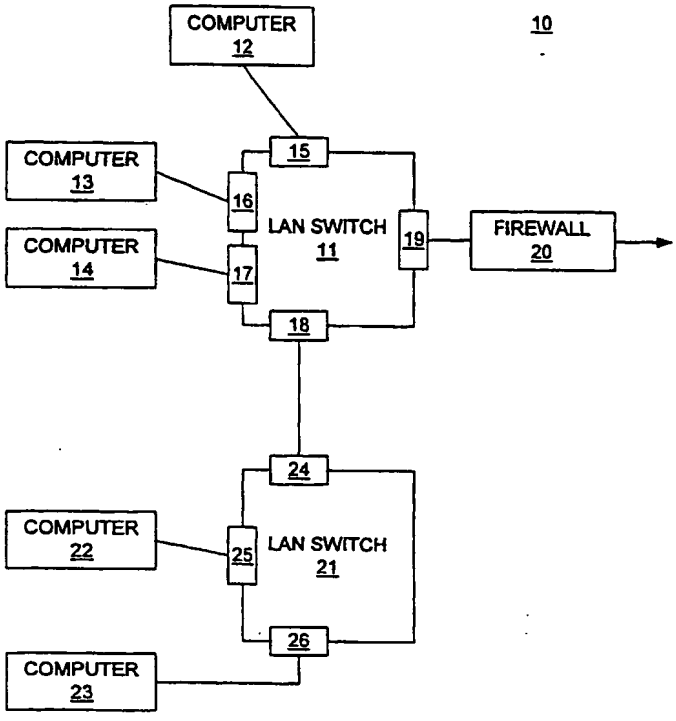
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE NETWORK SWITCH



(57) Abstract: A secure network having means for controlling the flow of packets within the network. In one embodiment, the network includes a plurality of network devices coupled together at a LAN switch. Each network device is physically connected to a port of the LAN. Each port has a packet filter which receives at least a portion of a packet arriving at the port and determines whether the packet is authorized to pass through the port and be routed to a destination address. The filters may use pattern matching or other techniques for determining whether packets satisfy applicable access rules. The access rules are determined by a system administrator and downloaded to the LAN switch for implementation by the filters. Each filter may implement a different set of access rules and the filters may be used by the administrator to set access levels for selected network devices or to isolate particular devices.

WO 01/06726 A2

TITLE: SECURE NETWORK SWITCH

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to computer networks and more specifically to means for filtering data packets transmitted through a LAN switch in a network in order to control access between individual computers and the remainder of the network.

2. Description of the Relevant Art

Rapid advances in computer technology and decreases in the cost of this technology have lead to widespread use of computers and computer networks. Likewise, organizations are increasingly relying on communications with computers outside their own networks. For example, organizations may need access to the World Wide Web to conduct research, send e-mail, and transfer files from one location to another. Similarly, web pages may be used to conduct marketing campaigns, distribute information, or establish a point of contact between a company and potential customers. Because of this increased exposure to computer systems and networks outside the organization's own network, security has become a growing concern. The exposure of the network to external entities provides many opportunities for wrongdoing such as unauthorized accesses or attacks on the network.

As security concerns have increased, it has become increasingly common for companies to implement firewalls between their internal networks and other, external networks. In fact, a firewall is generally considered a necessity for any company network which is connected to the internet. A firewall acts as a barrier between the network which serves the company or enterprise and external networks. The firewall serves as an inspection point through which all data must pass before it enters the internal network. As the data reaches the firewall, it is inspected to determine whether it meets one or more rules by which access to the internal network may be granted. These rules are programmed into the firewall by the system administrator. Firewalls are a convenient way to prevent many unauthorized accesses, or even attacks which may be attempted from outside the network. Firewalls are normally implemented at the only line of communication between the enterprise network and external networks. A system administrator thus has a central point at which he or she may examine incoming packets, enforce access rules, and monitor unauthorized activity.

While firewalls provide many security benefits, they have shortcomings as well. One such shortcoming is that, once an unauthorized access is made to the system, there is nothing that can be done by the firewall to contain the damage which may be caused by the access. Firewalls are also unable to prevent accesses which simply circumvent the firewall. For instance, if an enterprise network user is allowed to directly dial out of the network to an external system, data which passes through this connection will not be inspected and subjected to the firewall access rules. Firewalls are also powerless to prevent network users from bringing virus-infected floppy disks from external sources and loading them onto the network. If a virus infects one computer on the network, the virus can spread to the remainder of the network without having to pass the firewall. Still further, a firewall cannot prevent the damage which can be caused by the intrusion of a hostile machine within the firewall.

SUMMARY OF THE INVENTION

One or more of the problems described above may be solved by the various embodiments of the present invention. The invention implements means within an enterprise computer network for controlling the flow of data packets within the network. ("Enterprise" is used here to mean a network which serves a business or enterprise -- it is intended to indicate a point of reference and is not designate to indicate a particular type of network.) These means are implemented independently of a firewall, which controls the flow of packets only between the enterprise network and an external network such as the internet. Thus, even if unauthorized packets defeat or somehow circumvent the firewall, they may be prevented from affecting devices on the enterprise network by virtue of the invention.

In one embodiment, several computers are coupled together in a network by a LAN (Local Area Network) switch. (Unless otherwise specified, the term "computer" as used in connection with networks herein refers to any device which may be connected to a network and which is configured to transmit and/or receive packets, e.g., workstations, printers, file servers, modem servers, routers, etc. Similarly, the term "LAN switch" refers to any type of interface device for devices on a network, such as switches, routers and hubs.) The LAN switch has several physical ports and each of the computers is connected to one of the ports. A packet filter is associated with each of the ports. The packet filter defines the type of packets which are and are not allowed to pass through the port to and from the associated computer. When a packet is received by one of the ports, the associated filter is used to determine (e.g., by packet-matching) whether the packet should be transmitted to the computer for which it is destined or whether some other action should be taken. This alternate action may consist of dropping the packet, rerouting the packet to another port, or simply notifying the system administrator of the packet. The ports can thereby be used to physically control access to their respective lines and the computers coupled thereto.

In one embodiment, the packet filters scan the packets in parallel with the normal processing (e.g., addressing) of the packets. This normal processing typically consists of determining a destination address for the packet. The filters can perform packet matching (comparing certain fields in the packet with predetermined patterns) to determine whether the packets are authorized. If it is determined that a packet is unauthorized, the filter sends a signal to the LAN switch so that the packet can be dropped or rerouted before it gets beyond the LAN switch. By performing the packet filtering in parallel with the normal processing, overhead and delays in the network are minimized.

In one embodiment, each packet filter is programmed by a software executive running on the LAN switch. The network administrator can download permissions for each of the respective packet filters. The network administrator can thereby control access at each one of the ports in the same manner as with a firewall. Because the packets are independently filtered at each port, however, the network administrator can configure the access rules differently for each computer. The network administrator can thereby set up different classes of users or even isolate individual computers from the remainder of the network.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects and advantages of the invention will become apparent upon reading the following detailed description and upon reference to the accompanying drawings in which:

Fig. 1 is a block diagram illustrating a computer network in one embodiment of the invention.

Fig. 2 is a flow diagram illustrating the paths which packets may traverse from a source computer to a destination computer.

Fig. 3a is a functional block diagram of one port of a packet-filtering LAN switch in one embodiment of the invention.

Fig. 3b is a functional block diagram of one port of a packet-filtering LAN switch in an alternate embodiment of the invention.

Fig. 3c is a functional block diagram of one port of a packet-filtering LAN switch in an alternate embodiment of the invention.

Fig. 3d is a block diagram of a CPU and a plurality of ports of a packet-filtering LAN switch in one embodiment of the invention.

Fig. 4 is a flow diagram illustrating the operation of a LAN switch in one embodiment of the invention.

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof are shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that the drawing and detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the intention is to cover all modifications, equivalents and alternatives falling within the spirit and scope of the present invention as defined by the appended claims.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

One embodiment of the invention is described in detail below. This embodiment is implemented in a network of interconnected computers. Each of the computers is connected to the network via a LAN switch. ("LAN switch" as used herein means any device which forwards packets to computers in a network.) The LAN switch has a number of ports to which the computers are connected. When a packet is sent to one of the computers on the network, the packet is sent first to the LAN switch. The LAN switch processes the packet and determines where the packet should be sent next if it is normally routed.

In addition to this normal routing, however, the LAN switch needs to examine the packet to determine whether it should be normally routed. The LAN switch therefore includes a filter at each port. The filter is applied against the state of certain bits in the packet. Particular states are allowed in packets destined for a particular computer or group of computers, while others are not. If the bits are in an allowed state, the packet is routed in the normal manner to the destination computer. If the bits are in a state which is not allowed, the packet is not routed in the normal manner. For example, it may simply be dropped, or it may be rerouted to another computer. As another example, the packet may be routed to the destined computer, but the system administrator may be notified of the packet.

In one embodiment, the LAN switch executes a software executive that controls the filters. The system administrator uses the software executive to configure the filter for each of the computers. The filters can be individually configured so that there are different access rules for the different computers. The system administrator can thereby set up groups of computers which have different levels of access to network resources, restrict particular actions to certain computers, or isolate individual computers in order to handle problems relating specifically to those computers.

Fig. 1 is a block diagram illustrating a computer network 10. Network 10 includes several computers 12-14, each of which is coupled to LAN switch 11. The computers are coupled to the LAN switch through ports 15-17. Network 10 also includes computers 22 and 23, which are coupled to LAN switch 11 via a second LAN switch 21 and associated ports 24-26. Network 10 is coupled to external networks through LAN switch 11, port 19 and firewall 21. In many instances, the external network will be the internet. It should be noted that many different types of network devices are known to persons of skill in the art and any such devices can be coupled to the network in addition to, or in place of, computers 12-14 and 22-23. Further, network 10 is one of many potential network configurations and it is contemplated that the invention could be implemented in any one of these potential configurations. Network 10 may itself comprise several networks. For example, Fig. 1 depicts a network consisting of two sub-networks, one formed by LAN switch 11 and computers 12-14, and the other formed by LAN switch 21 and computers 22-23.

Computers 12-14 can communicate with each other and with computers on other networks using packet switching protocols. (As noted above, "computer" includes various types of network devices.) Packet switching protocols require that information to be sent between two computers be divided into packets. These packets are then transmitted between the computers. This is in contrast to a circuit switching protocol, which establishes a dedicated connection between the computers over which information can be transmitted without first being packetized. Networks using packet switching protocols may establish a virtual connection between the two computers instead of a physical connection. The virtual connection does not require intermediate lines to be dedicated to transmission of the packets. The packetization of the information therefore allows information to be sent across many intermediate networks without tying up their circuits and preventing communication between other computers.

Because information transmitted between two computers is divided into packets, the computers between the source and destination must have some way to determine where to send the packets. Each packet therefore includes a destination address. In many networks, an IP (Internet Protocol) address or TCP/IP (Transport Control Protocol /Internet Protocol) address is used. The IP address contains four bytes separated by periods (e.g., "012.123.234.001".) This address may specify a particular computer or it may specify a particular network, in which case the network will provide means to correctly route the packet to the correct device on that network. The TCP protocol exists at a slightly higher level than the IP protocol and provides means for ensuring that all of the bytes in message are received at the destination device. The TCP protocol sequences the bytes in a message and provides for retransmission of lost bytes.

Fig. 2 illustrates a series of interconnected computers (or networks) which form a path from a source computer 40 to a destination computer 41. In the figure, the source and destination computers are each depicted as being connected to the other computers through another device 42, 43. It will be assumed for the purposes of this discussion that devices 42 and 43 are firewalls. These devices may be other devices, such as LAN switches or computers, in other embodiments. The dashed lines indicate the boundaries of a source network 44 and destination network 45. When source computer 40 sends a packet to another computer, it is normally routed by a number of intermediate computers 51-55. These intermediate computers are typically routers. (Although "router" may be used to refer to a specific type of packet-forwarding device, the term as used here means any device which serves to route or forward packets between computers.) These routers examine the destination address of the

packet and determine the next router to which the packet will be sent. This process is repeated for each packet in a message. The process is typically performed independently for each packet so that the packets corresponding to a single message may travel from the source computer to the destination computer over a number of different routes. For example, one packet may be passed from the source network to 54 to 53 to 55 to the destination network, while another packet may be passed from 51 to 52 to 45. When the packets arrive at the destination network, they are directed to the destination computer. At the destination computer, the packets are re-assembled into the original message.

When a packet reaches the destination network, which in this case employs a firewall, it must pass through the firewall before it can be delivered to the destination computer. The firewall is typically a computer which is dedicated to the task of examining packets which arrive at the network to determine whether they are authorized to be distributed within the network. Firewalls may use various techniques to prevent unauthorized packets from gaining access to the network. These techniques may include the use of packet filters, application gateways and circuit-level gateways. Firewalls may be very effective in protecting the system against unwanted accesses, but this protection is not foolproof and unauthorized packets may be introduced into the network. Once the packets have breached the firewall, the firewall is completely ineffective to prevent the packets from being freely transmitted within the network. The firewall is also incapable of preventing users within the network from circumventing the firewall by dialing out on a telephone line or using portable media (e.g., floppy disks) to download unauthorized files onto the network. The invention is therefore implemented in this embodiment in one or more LAN switches through which all of the traffic internal to the network is routed.

After a packet passes through the firewall, it must be routed by the LAN switch to the appropriate computer on the network. When the LAN switch receives the packet, the switch must process it to determine its destination address in the same manner as other routing devices. In addition to routing the packet, the LAN switch performs a function similar to that of the firewall, rejecting or rerouting some and allowing others to pass. The LAN switch thereby controls the flow of packets within the network. Because the computers on the network are connected to each other through the switch, it can control the packet flow to and from each computer to which it is connected. Thus, even if an unauthorized packet passes through the firewall (either by circumventing it or defeating it), the packet must still satisfy the access rules of the LAN switch before it can be transmitted from one device to another within the network.

Fig. 3a is a functional block diagram of one port of the packet-filtering LAN switch. LAN switch 30 contains circuitry 31 for processing packets and determining their respective destinations on the network. LAN switch 30 also includes filter circuitry 32 which examines the packets to determine whether they are authorized to be routed to their destinations. Because of the distributed nature of the filtering (it is performed at each port of the LAN switch), filter circuitry 32 may implement access rules which are simpler than those implemented in a firewall. In other words, because each filter controls access to a single computer, only the rules relevant to that computer need to be implemented. These simplified access rules may, in many respects, be just as effective as those of the firewall because the rules implemented in a single filter can be tailored to the single computer associated with that filter. The distributed nature of the filtering also allows the network to be easily scalable. In other words, as computers are added to the network, corresponding filters are added to handle the filtering workload. The distribution of the filtering among the ports of the LAN switch allows the high volume of traffic

within the network to be filtered. (The implementation of a centralized, firewall-type system inside the network might reduce performance -- the firewall is more suitable for filtering packets coming into and going out of the network, which generally comprise a much lower volume of traffic than that internal to the network.)

As shown in Fig. 3a, incoming packets which arrive at a port of the LAN switch are delivered to both address processing circuitry 31 and the filtering circuitry 32. (It is contemplated that other embodiments could provide for delivery of only a portion of the packet (e.g., the packet header) to filtering circuitry 32.) Although the figure depicts the packets as exiting port 30 to the computers, the system can be applied to either outgoing or incoming packets. The packets are filtered in parallel with the normal address processing. As a result, the time required to perform the filtering is overlapped with the time required for normal address processing. Consequently, the overhead relating to the filtering is reduced. (It is contemplated that the filtering of the packets may be performed in series with the address processing as shown in Figs. 3b and 3c, but this would result in higher overhead and therefore is not the preferred embodiment. Figs. 3b and 3c illustrate that the serial filter circuitry may be located either before or after the address circuitry.)

Address processing circuitry 31 provides its output to switching circuitry 33. Switching circuitry 33 would, in the absence of the invention, use the destination address from address processing circuitry 31 to deliver the packet to its destination. The delivery of the packet, however, is conditioned upon the output of filtering circuitry 32. Filtering circuitry 32 applies the appropriate access rules to the packet and provides a signal to switching circuitry 33. If the packet is authorized to be delivered to its destination, a corresponding signal is input to switching circuitry 33 and the packet is forwarded to the destination in the normal manner. If the packet is not authorized, a different signal is produced by filtering circuitry 32. Upon receipt of this signal, switching circuitry 33 takes some alternate action. This alternate action may be any appropriate action relating to the presence of the unauthorized packet, and may include dropping the packet, rerouting the packet to an alternate destination, notifying the system administrator, or similar actions. The selected action for an unauthorized packet may depend on the particular destination of the packet, the type of packet, the application associated with the packet or other information.

Because the address and filtering circuitry at each port is normally kept to a minimum in order to maximize the throughput of the port, some complex operations may be delegated to a CPU in the LAN switch (see Fig. 3d.) For example, the filter circuitry is typically sufficient to perform pattern matching, but the implementation of more sophisticated filtering rules is beyond its capabilities. If the filter circuitry at one of ports 30 receives a packet which it doesn't recognize or can't properly filter, it can send the packet to the CPU 35 for processing. CPU 35 can then send the appropriate signal to the filer circuitry or switching circuitry at the respective port to process the packet. The circuitry in the port may also be limited in the actions it may perform in regard to processing the packet (e.g., forwarding or dropping the packet) and may delegate more complex actions to the CPU.

Fig. 4 is a flow diagram illustrating the operation of the LAN switch. This figure summarizes the operation of the LAN switch in one embodiment of the invention. When the packet is received at a port of the LAN switch 60, it is simultaneously processed to determine its destination address 61 and filtered to determine whether it satisfies the port's access rules 62. If the packet satisfies the access rules 63 and is authorized to be forwarded, the LAN switch forwards the packet to its destination 64 in the same manner as if it were not filtered.

If the packet fails to satisfy the excess rules 63 and is therefore not authorized, the packet is dropped 65. In other embodiments, unauthorized packets may be handled in a variety of ways. For example, they may be rerouted to an alternate destination, or they may be forwarded to the computer at the destination address while notification of the packet is sent to the system administrator.

In one embodiment, the filtering circuitry in the LAN switch is programmable. The network administrator determines the access rules to be applied in the filter and programs those rules into the filter. The filtering rules are based on the information in the header of the packet. This information is used because it is available for the normal forwarding of the packets. The information may include the IP source and destination addresses, the encapsulated protocol (e.g., TCP), the TCP/IP source and destination ports, the ICMP (Internet Control Message Protocol) message type, and the incoming and outgoing interfaces of the packet. The filtering rules may be of various types and implementations. For example, rules may be service-dependent (e.g., allowing incoming FTP sessions only to certain computers) or service-independent (dropping packets having internal IP addresses, but which appear on external ports).

In one embodiment, the filter is implemented using the Java programming language. Java was chosen for this implementation because Java virtual machines exist for many platforms and Java applications can therefore be run on these many platforms. A Java-based filtering application thus has a degree of platform and/or vendor neutrality. (It is contemplated, however, that the filtering application may use any suitable programming language.) In this implementation, a software executive is executed in filtering circuitry 32. The software executive is an application which provides a framework for implementation of the system administrator's rules. The system administrator determines which rules should be applied to packets entering the LAN switch and configures Java applets which, in conjunction with the software executive, implement these rules. (Applets are small Java applications.) The Java applets are downloaded by the system administrator from one of the computers on the network to the LAN switch. The applets are then called by the software executive when a packet must be filtered.

Various embodiments of the invention may allow users to overcome problems found in networks which do not incorporate the invention. For example, as set forth above, packets which are routed from a source computer to a destination computer may have to traverse several networks which lie between the computers. Each time one of the packets arrive at one of these networks, the network (i.e. a router within the network) must read the packet's address information and determine an intermediate device to which the packet will be sent for further forwarding. The determination of where the packet should be sent is based upon information provided to the routing device by other computers. If one of these computers provides inaccurate information to the routing device, the packet may be incorrectly routed.

It is not unusual to find a computer which has a particular address, but which broadcasts to other devices that it has a different address. A router may rely on this information and may determine that the shortest route to the destination computer goes through the computer which broadcast the incorrect address. The router may then forward packet to this computer using the incorrect address which provided. The computer which broadcast the incorrect information, however, will not recognize the address to which the packet was forwarded and will simply drop the packet. In this scenario, the computer which broadcast the incorrect address information has effectively created a dead end or "black hole" into which forwarded packets will simply disappear.

If the system administrator becomes aware of this problem, he or she may wish to isolate the offending computer from the remainder of the network in order to prevent more packets from being lost. In one embodiment of the invention, the system administrator can configure the filter associated with the computer so that no incoming or outgoing packets are allowed to pass through the associated port of the LAN switch. The system administrator thereby prevents the computer from sending out incorrect address information and also prevents packets from being passed to the computer and lost. This method of isolating the offending computer also has the benefit of not requiring physical access to the computer -- the isolation is achieved by reconfiguration of the filter associated with the computer. In a situation where the computer is in a locked room or building, this may be the only means for isolating the computer.

As another example, many companies hire subcontractors to perform work on the various projects. This work may involve software development, design analysis or other tasks which necessitate use of or access to computers on the company's network. The company, however, may not wish for these subcontractors to have access to applications or data which are not related to the tasks being performed by the subcontractors. In one embodiment of the invention, the system administrator may configure the filters associated with the computers used by the subcontractors to prevent access to the restricted data or applications. For example, a filter associated with a computer containing sensitive data may be configured to drop packets received from certain computers which are being used by the subcontractors. Likewise, the filter can be configured to prevent packets from being delivered to these computers. By properly configuring the filters on the LAN switch, the system administrator can set up various privilege levels for subcontractors, employees, executives and other system users.

While the present invention has been described with reference to particular embodiments, it will be understood that the embodiments are illustrated and that the invention scope is not so limited. Any variations, modifications, additions and improvements to the embodiments described are possible. These variations, modifications, additions and improvements may fall within the scope of the invention as detailed within the following claims.

WHAT IS CLAIMED IS:

1. A secure computer network comprising:

a network interface device having a plurality of ports;

a plurality of network devices coupled to said ports; and

a plurality of filters, each said filter coupled to a corresponding one of said ports to receive data packets arriving at said one of said ports;

wherein said each filter is configured to examine said data packets and to determine whether said data packets satisfy a set of access rules;

wherein said each filter is further configured to convey a signal to said network interface device indicating whether said data packets satisfy said set of access rules; and

wherein said network interface device is configured to take a predetermined action with respect to each of said data packets for which said signal indicates said each packet fails to satisfy said set of access rules.

2. The secure network of claim 1 further comprising a firewall between said secure network and an external network.

3. The secure network of claim 1 wherein said network interface device performs processing on said packets, said processing comprising examining each said packet to determine a corresponding destination address.

4. The secure network of claim 3 wherein each said filter is configured to examine said data packets in parallel with said processing performed by said network interface device.

5. The secure network of claim 4 wherein each said filter is configured to determine whether said data packets satisfy a set of access rules by performing packet matching on said packets.

6. The secure network of claim 1 wherein said predetermined action is selected from the group of actions consisting of: dropping said packet; rerouting said packet; and reporting said packet.

7. The secure network of claim 1 wherein said network interface device is configured to execute a software executive and wherein said access rules of said filters are set according to program code which is downloaded to said software executive executing on said network interface device.

8. The secure network of claim 1 wherein a first one of said filters provides access to a first one of said network devices according to a first set of access rules, wherein a second one of said filters provides access to a second one of said network devices according to a second set of access rules, and wherein said first set of access rules is different from said second set of access rules.

9. The secure network of claim 1 wherein said network interface device comprises a LAN switch.

10. A method for controlling access between devices in a computer network, each of said devices being coupled to a corresponding port of a LAN switch, communication with the devices being achieved by transmission of information packets to and from the devices, the method comprising:

examining each packet when said each packet arrives at one of said ports of said LAN switch;

determining whether said each packet satisfies one or more port access rules;

if said each packet satisfies said one or more port access rules, routing said each packet to a destination address associated with said each packet; and

if said each packet does not satisfy said one or more port access rules, taking a predetermined action.

11. The method of claim 10 further comprising determining routing information for said each packet in parallel with determining whether said each packet satisfies said one or more port access rules.

12. The method of claim 11 wherein said predetermined action is selected from the group consisting of: dropping said each packet; rerouting said each packet; and reporting said each packet.

13. The method of claim 12 wherein determining whether said each packet satisfies said one or more port access rules comprises matching said each packet with one or more predetermined bit patterns and determining whether said patterns match said each packet.

14. The method of claim 12 wherein said port access rules comprise a first set of port access rules associated with a first one of said devices and a second set of port access rules associated with a second one of said devices.

15. The method of claim 12 further comprising examining one or more of said packets at a firewall and determining whether said one or more packets satisfy one or more firewall access rules.

16. A LAN switch for controlling the transmission of packets in a secure computer network comprising:

a plurality of ports wherein each of said plurality of ports is configured to be coupled to a corresponding network device; and

a plurality of filters, wherein each of said plurality of filters is coupled to a corresponding one of said plurality of ports and configured to pass packets which satisfy one or more access rules and to prevent passage of packets which fail to satisfy said one or more access rules.

17. The LAN switch of claim 16 wherein each of said filters is programmable by a system administrator to implement a first set of access rules for a first subset of said plurality of ports and a second set of access rules for a second subset of said plurality of ports, said first set of access rules being distinct from said second set of access rules.

18. The LAN switch of claim 16 wherein each of said plurality of ports comprises:

address processing circuitry configured to determine destination addresses associated with said packets; and

switching circuitry configured to route said packets.

19. The LAN switch of claim 18

wherein each of said filters is configured to generate a signal indicative of whether said packets satisfy said access rules to provide said signal to said switching circuitry of said corresponding port and

wherein said switching circuitry is configured to route said packets to said destination addresses if said signal indicates that said access rules are satisfied and to take an alternate action if said signal indicates that said access rules are not satisfied

20. The LAN switch of claim 19 wherein said alternate action is selected from the group consisting of: dropping said packets; routing said packets to an alternate destination; and transmitting a notification of said packets.

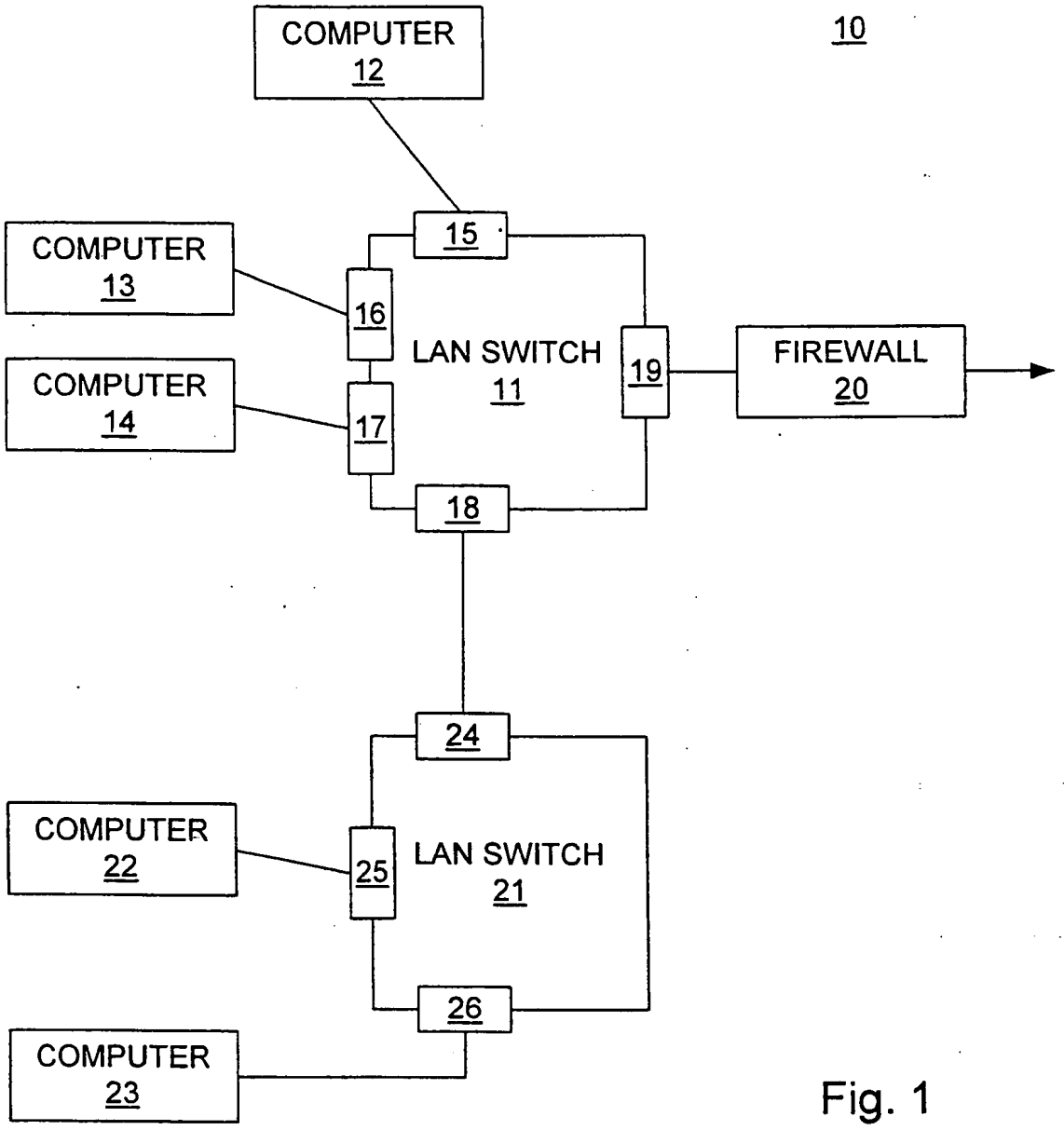


Fig. 1

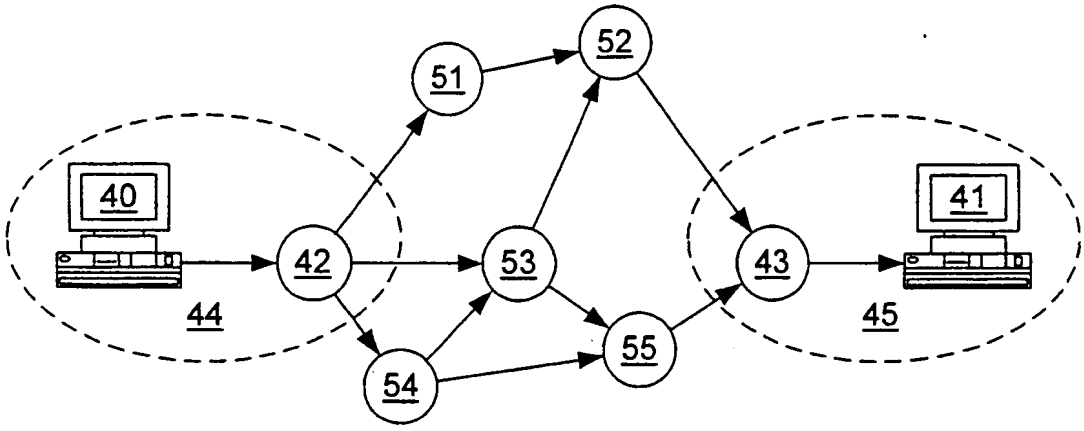

52
51
40
41
42
53
43
44
45
55
54

Fig. 2

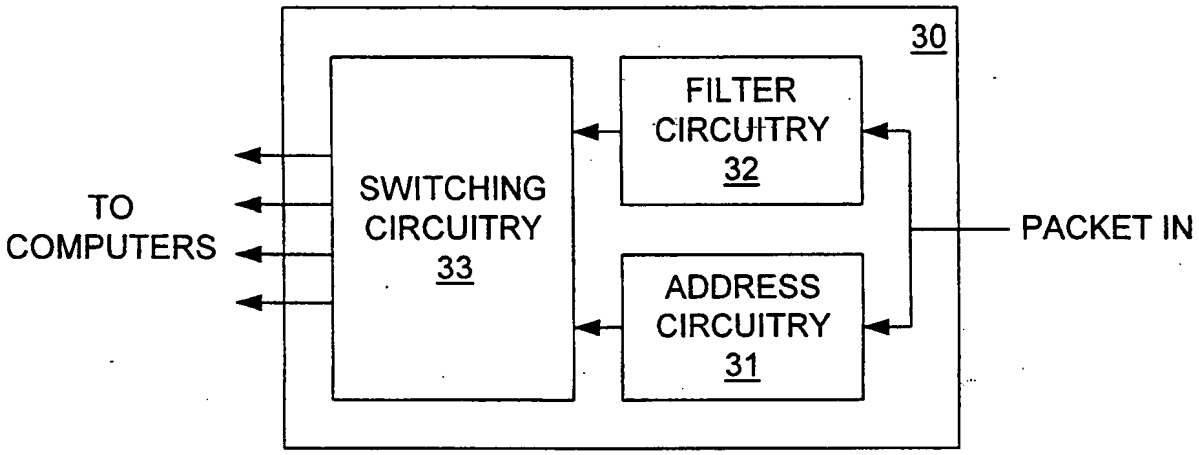

30
FILTER CIRCUITRY 32
SWITCHING CIRCUITRY 33
ADDRESS CIRCUITRY 31
TO COMPUTERS
PACKET IN

Fig. 3a

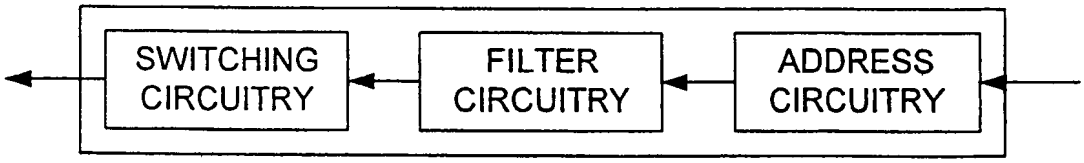


Fig. 3b

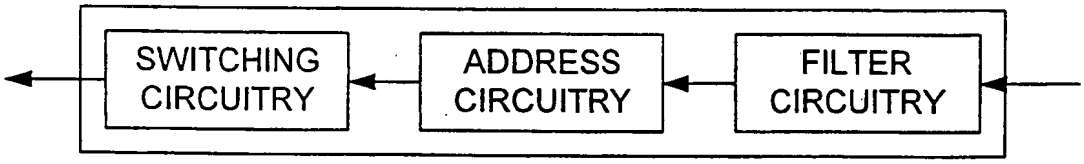


Fig. 3c

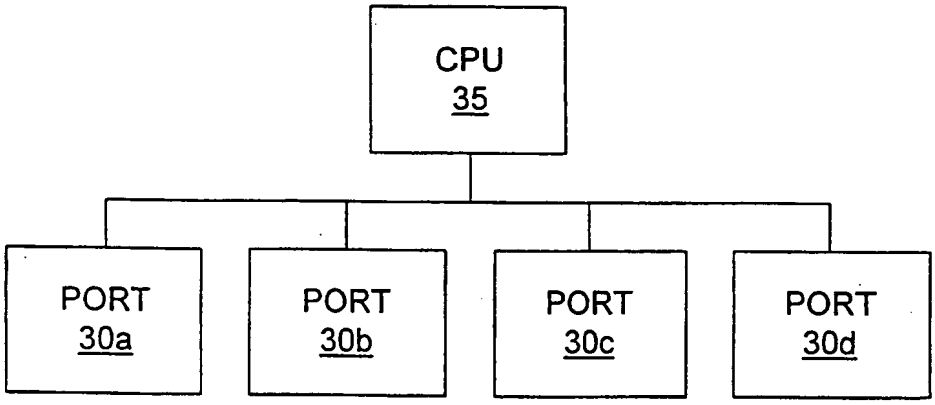


Fig. 3d

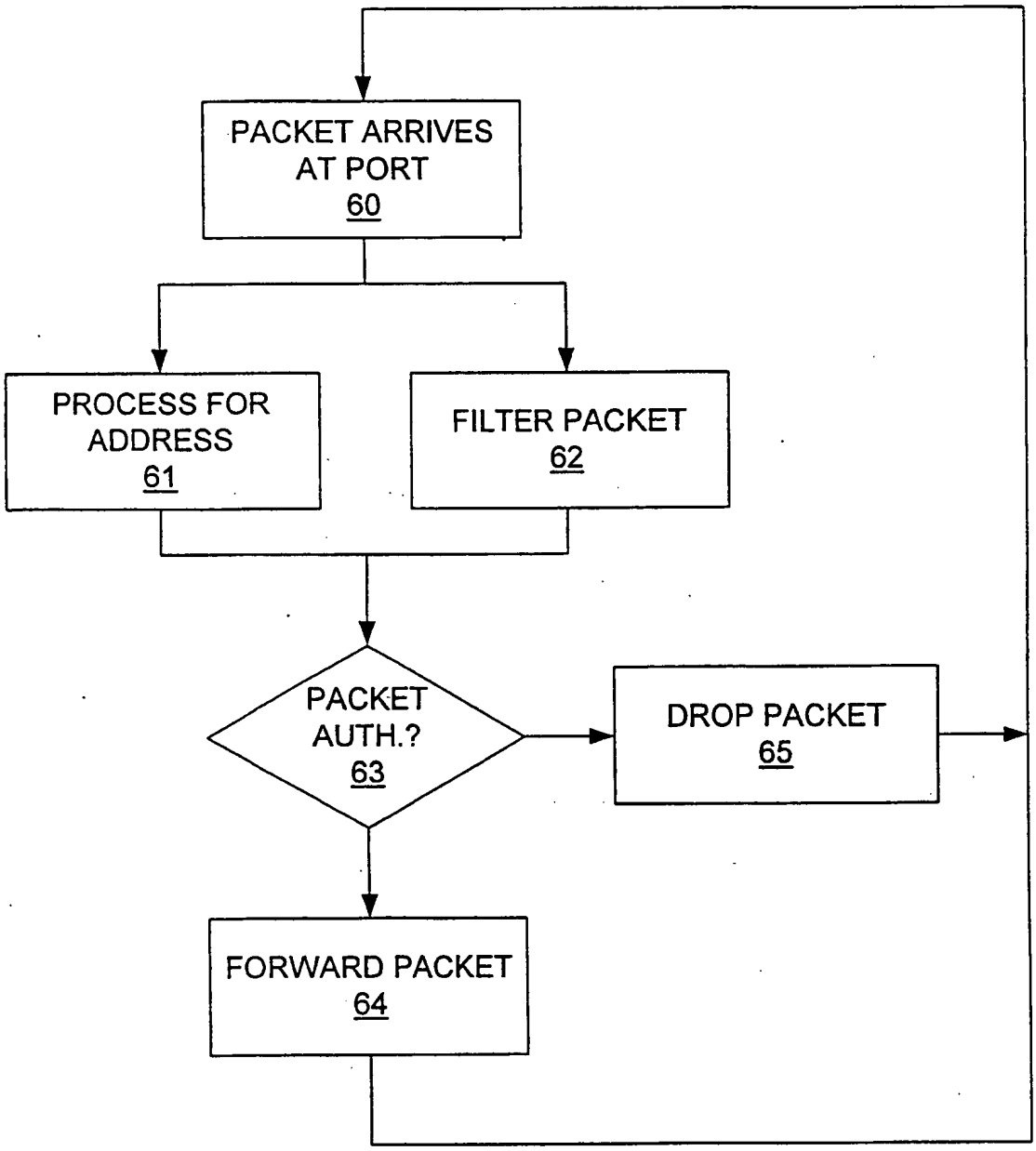

PACKET ARRIVES AT PORT 60
PROCESS FOR ADDRESS 61
FILTER PACKET 62
PACKET AUTH.? 63
DROP PACKET 65
FORWARD PACKET 64

Fig. 4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 January 2001 (25.01.2001)

PCT

(10) International Publication Number
WO 01/06726 A3

(51) International Patent Classification[7]: H04L 12/44, 29/06

(21) International Application Number: PCT/US00/18988

(22) International Filing Date: 12 July 2000 (12.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/354,294 15 July 1999 (15.07.1999) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventors: JOHNSON, John; 1061 Regency Knoll Drive, San Jose, CA 95129 (US). OKIN, Ken; 14880 Sobey Road, Saratoga, CA 95070 (US). RADUCHEL, William; 3111 Alexis Drive, Palo Alto, CA 94304 (US).

(74) Agent: KIVLIN, B., Noel; Conley, Rose & Tayon, P.C., P.O. Box 398, Austin, TX 78767-0398 (US)..

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

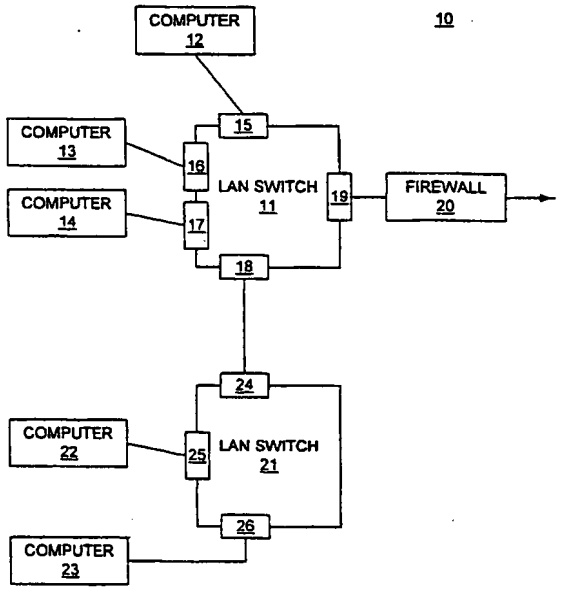
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
25 April 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE NETWORK SWITCH



(57) Abstract: A secure network having means for controlling the flow of packets within the network. In one embodiment, the network includes a plurality of network devices coupled together at a LAN switch. Each network device is physically connected to a port of the LAN. Each port has a packet filter which receives at least a portion of a packet arriving at the port and determines whether the packet is authorized to pass through the port and be routed to a destination address. The filters may use pattern matching or other techniques for determining whether packets satisfy applicable access rules. The access rules are determined by a system administrator and downloaded to the LAN switch for implementation by the filters. Each filter may implement a different set of access rules and the filters may be used by the administrator to set access levels for selected network devices or to isolate particular devices.

WO 01/06726 A3

INTERNATIONAL SEARCH REPORT

Internat I Application No
PCT/US 00/18988

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/44 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 790 554 A (FERGUSON EARL ET AL) 4 August 1998 (1998-08-04)	1,3,6, 8-10, 16-20
Y	column 6, line 21 - line 65 column 9, line 5 - line 42	2,4,5,7, 11-15
X	US 5 568 613 A (FUTRAL WILLIAM T) 22 October 1996 (1996-10-22)	1,3, 8-10, 16-19
A	column 4, line 1 - line 41 column 11, line 15 -column 12, line 16	2,4,6,7, 11,20
Y	US 5 835 726 A (DOGON GIL ET AL) 10 November 1998 (1998-11-10) column 5, line 55 -column 6, line 54; figure 16	2,7,15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 January 2001	26/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	RAMIREZ DE AREL.., F

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 899 333 A (ROEDIGER GARY A) 6 February 1990 (1990-02-06) column 2, line 59 -column 3, line 4	4,5, 11-15
A	US 5 559 883 A (WILLIAMS RICHARD) 24 September 1996 (1996-09-24) column 4, line 6 - line 54	1,3,4, 10,11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat Application No
PCT/US 00/18988

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5790554 A	04-08-1998	NONE	
US 5568613 A	22-10-1996	US 5638515 A	10-06-1997
US 5835726 A	10-11-1998	US 5606668 A	25-02-1997
		AU 6135696 A	15-01-1997
		CA 2197548 A	03-01-1997
		EP 0807347 A	19-11-1997
		WO 9700471 A	03-01-1997
		JP 10504168 T	14-04-1998
		NO 970611 A	15-04-1997
		CA 2138058 A	16-06-1995
		DE 69425038 D	03-08-2000
		EP 0658837 A	21-06-1995
		JP 8044642 A	16-02-1996
US 4899333 A	06-02-1990	CA 1321818 A	31-08-1993
		DE 68925830 D	11-04-1996
		DE 68925830 T	17-10-1996
		EP 0336598 A	11-10-1989
		HK 145696 A	09-08-1996
		JP 2013047 A	17-01-1990
		JP 2594640 B	26-03-1997
		SG 43795 A	14-11-1997
US 5559883 A	24-09-1996	NONE	